IN THE CLAIMS:

Please cancel claim 15 without prejudice:

1. (Previously Amended) A storage medium data protecting method of protecting data on a storage medium, comprising:

a step of generating random key data, encrypting the key data with a password, and writing the encrypted key data to said storage medium;

a step of encrypting the data with the generated random key data, and writing the encrypted data to said storage medium;

a step of reading the encrypted key data from said storage medium;

a step of decoding the encrypted key data with the password; and

a step of decoding the data on said storage medium with the decoded key data,

wherein said key data generating step comprises:

a step of generating different random key data for each of a plurality of unit storage areas of said storage medium;

a step of encrypting each said different random key data for each unit storage area with said password, and

a step of writing each said encrypted key data to said storage medium,

wherein said data encrypting step comprises a step of encrypting the data with the random key data corresponding to said unit storage area to write the data, and

wherein said data decoding step comprises a step of decoding the data with the decoded key data corresponding to said unit storage area where the data have been read.

2. (Original) A storage medium data protecting method according to claim 1, wherein said key data generating step comprises a step of generating the key data per logic sector on said storage medium.

3. (Previously Amended) A storage medium data protecting method according to claim 1, wherein said key data generating step comprises a step of generating is different key data for each writing to said unit storage areas.

4. (Original) A storage medium data protecting method according to claim 1, wherein said key data generating step comprises a step of generating the key data by combining a predetermined number of pieces of random data.

5. (Original) A storage medium data protecting method according to claim 1, further comprising:

a step of decoding, after reading the encrypted key data from said storage medium, the encrypted key data with an old password designated by a user; and

a step of writing, after encrypting the decoded key data with a new password designated by the user, the encrypted key data to said storage medium.

6. (Original) A storage medium data protecting method according to claim 1, wherein said step of writing the encrypted key data to said storage medium comprises a step of encrypting the key data with each of a plurality of passwords, and writing the encrypted key data to said storage medium, and

said step of decoding the key data comprises a step of decoding the read/encrypted data with a password designated.

7. (Previously Amended) A storage medium data protecting method according to claim 1, wherein said step of writing the encrypted key data to said storage medium comprises a step of encrypting the key data with a first password, writing the encrypted key data to said storage medium, encrypting said first password with a second password, and writing said first encrypted password, and

said step of decoding the key data comprises a step of decoding said first encrypted password with said second password, and obtaining said first password, and a step of decoding the encrypted key data with said first password.

8. (Previously Amended) A storage medium data protecting apparatus for protecting data on a storage medium, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating random key data, the random key data with a password, writing the encrypted key data to said storage medium, encrypting the data with the key data, and writing the encrypted data to said storage medium;

a read mode of encoding, after reading the encrypted key data from said storage medium, the encrypted key data with the password, and decoding the data on said storage medium with the decoded key data,

wherein said write mode comprises a mode of generating different random key data for each unit storage area of said storage medium, encrypting each said different random key data for each unit storage area with said password, writing each said encrypted key data to said storage medium, and encrypting the data with the random key data corresponding to said unit storage area to write the data,

wherein said read mode comprises a mode of decoding the data with the decoded key data corresponding to said unit storage area where the data have been read.

9. (Original) A data protecting apparatus according to claim 8, wherein said storage medium is constructed of a storage medium from and to which the data is read and written per logic sector, and

said control circuit generates the key data per logic sector on said storage medium.

10. (Previously Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit generates different key data for each writing to said unit storage areas.

11. (Original) A data protecting apparatus according to claim 8, wherein said generates the key data by combining a predetermined number of pieces of random data.

12. (Original) A data protecting apparatus according to claim 9, wherein said control circuit decodes, after reading the encrypted key data from said storage medium, the encrypted key data with an old password designated by a user, and writes, after encrypting the decoded key data with a new password designated by the user, the encrypted key data to said storage medium.

13. (Original) A storage medium data protecting apparatus according to claim 8, wherein said control circuit has:

a write mode of encrypting the key data with each of a plurality of passwords and writing the encrypted key data to said storage medium; and

a read mode of decoding the read/encrypted key data with the designated password.

14. (Previously Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit has:

a write mode of encrypting the key data with a first password, writing the encrypted key data to said storage medium, encrypting a second password with said first password, and writing said second encrypted password; and

a read mode of decoding said second encrypted password with said second password, obtaining said first password, and thereafter decoding the encrypted key data with said first password.

15. (Cancelled)

16. (Previously Added) The storage medium protecting method according to claim 1, said writing the encrypted key data step is performed for all unit storage areas of said storage medium when initializing said storage medium.

17. (Previously Added) The storage medium protecting method according to claim 16, said encrypting the data step comprises:

a step of reading the encrypted key data from said storage medium;

a step of decoding said read encrypted key data with said password; and

a step of encrypting the data with said decoded key data.

18. (Previously Amended) An encoding method protecting data on a storage medium, comprising:

a step of generating different random key data for each unit storage area of said storage medium, encrypting the random key data with a password, and writing the encrypted key data to said storage medium;

a step of encrypting the data with the random key data corresponding to said unit storage area to which the data is to be written, and writing the encrypted data to said storage medium.

19. (Previously Amended) A decoding of protected data on a storage medium having a plurality of unit storage areas, wherein different key data is used for each unit storage area and the different key data is encrypted with at least one password, comprising:

a step of reading the encrypted key data from said storage medium;

a step of decoding the encrypted key data with said at least one password; and

a step of decoding data on said storage medium with the decoded key data corresponding to the unit storage area where the data have been read.